DMP/JAS:AFM/EHS/BZM
F. #2019R00476

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

[redacted]

ARTEM ALEKSANDROVYCH STRYZHAK,

Defendants.

----------X

S U P E R S E D I N G
I N D I C T M E N T

Case No. 23-324 (S-1) (PKC)
(T. 18, U.S.C., §§ 371, 982(a)(2), 982(b)(1), [redacted] and 3551 et seq.; T: 21, U.S.C., § 853(p))

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Superseding Indictment, unless otherwise noted:

1. "Malware" was a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems and take other unauthorized action on a computer system. Common examples of malware included viruses, ransomware, worms, keyloggers and spyware.

2. "Ransomware" was a type of malware that infected a computer or computer network and encrypted some or all of the data. Distributors of ransomware typically extorted the user of the encrypted computer by demanding that the user pay a ransom in bitcoin to receive a decryption code and recover the data from the encrypted computer.

3. "Encryption" was the translation of data into a secret code. In order to access encrypted data, a user needed access to a password, commonly referred to as a "decryption key" or "decryptor," that enabled the user to decrypt the data.

4. "Bitcoin" (abbreviated as "BTC") was a type of virtual currency circulated over the Internet as a form of value. Bitcoin were not issued by any government, bank or company, but were generated and controlled through computer software operating via a decentralized, peer-to-peer network. To acquire bitcoin, typically a user purchased them from a bitcoin seller or "exchanger."

5. "Bitcoin addresses" were particular locations to which bitcoin were sent and received. A Bitcoin address was analogous to a bank account number and was represented as a 26-to-35 character, case-sensitive string of letters and numbers. Each Bitcoin address was controlled through the use of a unique corresponding private key that was a cryptographic equivalent of a password and was needed to access the Bitcoin address. Only the holder of a Bitcoin address's private key could authorize a transfer of bitcoin from that address to another Bitcoin address. Little to no personally identifiable information about a Bitcoin account holder was transmitted during a Bitcoin transaction.

6. "Tor" was a computer network designed to facilitate anonymous communication over the internet. Typically, user activities on the internet could be attributed to the user via Internet Protocol ("IP") addresses assigned by an internet service provider. The Tor network routed a user's communications through a globally distributed network of relay computers or proxies ("Tor network"), which typically prevented identification of users by IP address.

7. A "command and control server" or "C2 server" was a centralized computer that issued commands to remotely connected computers. "Command and Control" infrastructure consisted of servers and other technical infrastructure that issued commands to control malware.

8. "Cobalt Strike" was a commercial security testing tool that operated a command and control application with two primary components: the team server and the client. A team server accepted client connections. The client was used by operators to connect to the team server. "Beacon" was the name for Cobalt Strike's default simulated malware used to create a connection to the team server.

[redacted]

13. "Business Database-1," as used in this Superseding Indictment, refers to an online database of business and professional contact information, the identity of which is known to the Grand Jury.

[redacted]

15. "WinSCP" was a software program that allowed secure file transfers between a local computer and a remote server. At times, ransomware actors used WinSCP to exfiltrate data from computer networks without authorization.

I. The Defendants

[redacted]

17. The defendant ARTEM ALEKSANDROVYCH STRYZHAK ("STRYZHAK") was a citizen of Ukraine. STRYZHAK also used various online monikers.

II. The Ransomware Schemes

18. [redacted] Nefilim (at times, spelled "Nephilim") were forms, or strains, of ransomware that encrypted victim computers and computer networks.

19. From at least December 2018 to at least October 2021, [redacted] Nefilim ransomware were used to encrypt computer networks in countries around the world including the United States, Norway, France, Switzerland, Germany and the Netherlands, and including attacks against computers located in the Eastern District of New

York. These ransomware attacks caused extensive losses, resulting both from damage to victim computer systems and from ransomware payments to the perpetrators.

20. In these attacks, the perpetrators of [redacted] Nefilim typically customized the ransomware executable file (the ransomware file responsible for encryption) for each ransomware victim. The customization allowed the ransomware actors to create a decryption key that could only decrypt the network of the specific victim against which the ransomware was deployed and allowed ransomware actors to create customized ransom notes.

21. If the victims paid the ransom demand, the perpetrators would send a decryption tool, which enabled the victims to decrypt the computer files locked by the ransomware program.

22. As described further below, [redacted]

STRYZHAK used Nefilim malware to carry out ransomware schemes.

[redacted]

[redacted]

[redacted]

B. The Nefilim Scheme

34. From at least on or about July 1, 2020, through at least on or about October 26, 2021, [redacted] was one of the administrators of the Nefilim ransomware strain. [redacted] and the other Nefilim administrators provided other Nefilim ransomware actors, including STRYZHAK, with access to the Nefilim ransomware code in exchange for 20 percent of the ransom proceeds. The Nefilim administrators were responsible

for creating accounts for Nefilim affiliates to log in to the Nefilim panel, which served as a platform for Nefilim affiliates to access the Nefilim ransomware.

35. [redacted] used a virtual private server assigned an IP address ending in .15 ("Server 1") to access an instant messaging program that he used to coordinate with his co-conspirators, including STRYZHAK, in furtherance of the Nefilim ransomware conspiracy. [redacted] also stored at least three unique Nefilim ransomware files on Server 1.

36. [redacted] and his co-conspirators gained initial access to corporate victim networks in various ways, including by purchasing access to compromised networks, sometimes in return for a share of expected ransom proceeds.

37. At times, other cybercriminals approached [redacted] to learn more about joining the group responsible for Nefilim ransomware attacks. [redacted] at times responded that he and the other Nefilim administrators received 20 percent of the ransom proceeds for a given attack. In or about June 2021, STRYZHAK contacted [redacted] and agreed to work with [redacted] as an affiliate of Nefilim ransomware. [redacted] agreed to provide STRYZHAK with access to Nefilim ransomware in exchange for [redacted] and other Nefilim administrators receiving 20 percent of the ransom proceeds STRYZHAK extorted from Nefilim victims.

38. At [redacted]'s direction, an individual whose identity is known to the grand jury ("Co-Conspirator-1") created an account for STRYZHAK to access the Nefilim ransomware panel and thereafter, [redacted] provided STRYZHAK with access to the Nefilim ransomware panel.

39. [redacted] at times described his preferred ransomware targets as companies located in the United States, Canada or Australia with more than $100 million in annual revenue. In one such exchange with STRYZHAK in or about July 2021, [redacted] encouraged STRYZHAK to target companies in these locations with more than $200 million in annual revenue.

40. [redacted] and other administrators of the Nefilim ransomware strain researched companies to which they gained unauthorized access, including by using tools like Business Database-1 to gather information about the victim companies' net worth, size and contact information. They then used additional hacking tools to explore the victim networks, obtain persistent remote access, move laterally (i.e., access other systems within the computer or network) and escalate privileges (i.e., gain greater authority over the computer or network).

41. After gaining sufficient access to the victims' networks, [redacted], STRYZHAK and their co-conspirators exfiltrated data from victims' computer networks, including victims located in the United States, in furtherance of their scheme to extort ransom payments from victims.

42. [redacted], STRYZHAK and their co-conspirators deployed Nefilim ransomware. To deploy Nefilim ransomware, the conspirators typically established a connection to a C2 server running the Cobalt Strike application. The perpetrators then transmitted computer code to prepare the victim computers to receive the ransomware program and encrypt the files of the victim computer or computer network.

43. As part of the deployment of Nefilim ransomware, victims' files were encrypted and rendered inaccessible. [redacted], STRYZHAK and their co-conspirators typically left notes on the victims' computers stating that their files had been encrypted and that

sensitive information had been extracted. The notes also typically instructed the victims to email two encrypted files to the perpetrators at three email addresses provided in the notes. The Nefilim notes also typically threatened the victims that unless they came to an agreement with the ransomware actors, the stolen data would be published on publicly accessible "Corporate Leaks" websites, which were maintained by [redacted] and other co-conspirators.

44. After a victim sent two encrypted files, the Nefilim conspirators returned the files in decrypted form along with further instructions and demands, including a demand for a ransom payment.

45. Victims who paid the ransom typically received a decryption key for the locked data. When victims refused to pay, [redacted] and other co-conspirators published their exfiltrated data on the "Corporate Leaks" sites.

46. After ransom payments were received, [redacted] instructed co-conspirators on how to distribute the proceeds amongst the conspirators.

III. The Victims

47. [redacted], STRYZHAK and their co-conspirators attacked the computer systems of numerous victims around the United States and the world. Some of those victims, entities the identities of which are known to the Grand Jury, are described below:

(a) Victim 1 was an engineering consulting company located in France.

(b) Victim 2 was a company in the aviation industry located in the Eastern District of New York.

(c) Victim 3 was a chemical company located in the Southern District of Ohio.

(d) Victim 4 was an international eyewear company with computer servers located in the Eastern District of New York.

(e) Victim 5 was an insurance company located in the Central District of Illinois.

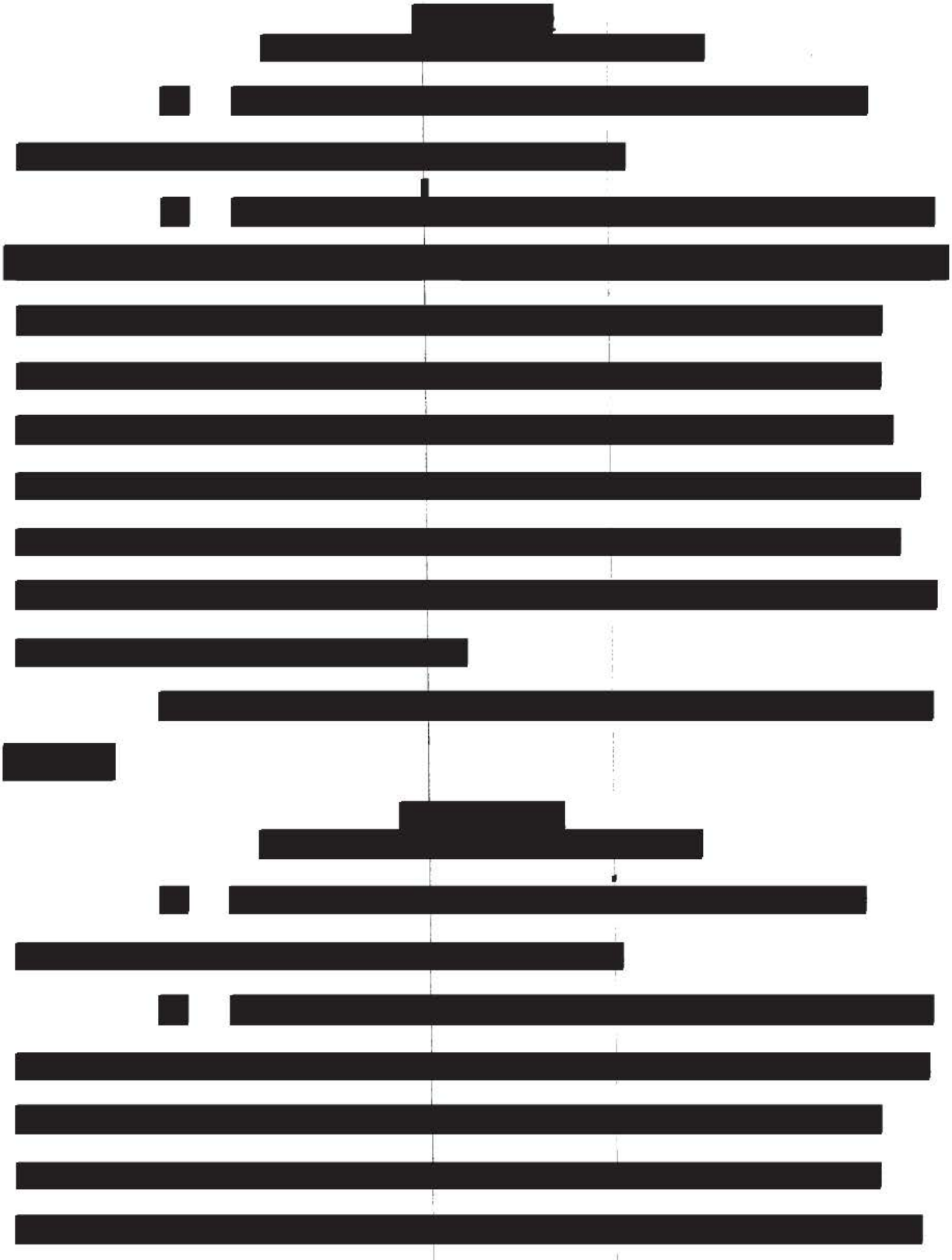
(f) Victim 6 was a company in the construction industry located in the Western District of Texas.

(g) Victim 7 was a company in the oil and gas transportation industry.

(h) Victim 8 was a company in the pet care industry located in the Eastern District of Missouri.

[redacted]

[redacted]



[redacted]

COUNT FIVE
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)
(Nefilim Conspiracy)

57. The allegations contained in paragraphs one through 47 are realleged and incorporated as if fully set forth in this paragraph.

58. From at least on or about July 1, 2020, through at least on or about October 26, 2021, within the Eastern District of New York and elsewhere, the defendants [redacted] and ARTEM ALEKSANDROVYCH STRYZHAK together with others, did knowingly and willfully conspire:

(a) to access a computer without authorization, and thereby obtain information from a protected computer, and (i) to commit the offenses for purposes of private financial gain, (ii) in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, to wit: transmitting in interstate and foreign commerce a demand in relation to damage to a protected computer, and (iii) to obtain information from the protected computer valued at more than $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), 1030(c)(2)(B)(ii) and 1030(c)(2)(B)(iii);

(b) to cause the transmission of a program, information, code and command, and as a result of such conduct, cause damage without authorization to a protected computer, and (i) cause loss to one or more persons during a one-year period from a course of conduct affecting one or more protected computers aggregating at least $5,000 in value, and (ii) cause damage affecting 10 or more protected computers during a one-year period, contrary to 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B); and

(c) with intent to extort from one or more persons any money and other things of value, to transmit in interstate and foreign commerce one or more communications containing one or more demands and requests for money and other things of value in relation to damage to a protected computer, which damage was caused to facilitate the extortion, contrary to 18 U.S.C. §§ 1030(a)(7)(C) and 1030(c)(3)(A).

59. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants [redacted] and ARTEM ALEKSANDROVYCH STRYZHAK, together with others, did commit and cause the commission of, among others, the following:

OVERT ACTS

(a) On or about September 19, 2020, [redacted] and other co-conspirators deployed Nefilim ransomware and encrypted computer networks of Victim 4. The affected computers included Victim 4 computers located in the Eastern District of New York.

(b) On or about September 19, 2020, [redacted] and these co-conspirators left a ransom note on Victim 4's computer servers demanding that Victim 4 contact the ransomware actors and threatening that if Victim 4 did not do so, the actors would leak exfiltrated data to a leak website.

(c) On or about October 18, 2020, following Victim 4's refusal to pay a ransom, [redacted] and these co-conspirators published approximately 102 GB of Victim 4 data on "Corporate Leaks" sites on Tor and elsewhere on the internet.

(d) On or about June 7, 2021, [redacted] and other co-conspirators encrypted Victim 5's networks using Nefilim ransomware.

(e) On or about June 22, 2021, STRYZHAK agreed with [redacted] to work as an affiliate of Nefilim ransomware. [redacted] provided STRYZHAK with access to Nefilim ransomware in exchange for [redacted] and other Nefilim administrators receiving 20 percent of ransom proceeds STRYZHAK extorted from Nefilim victims.

(f) On or about June 22, 2021, [redacted] informed STRYZHAK that STRYZHAK would need to have an account to access the Nefilim panel. [redacted] asked STRYZHAK what login username should be used for STRYZHAK's access to the Nefilim panel. STRYZHAK advised [redacted] to use his nickname. After confirming the nickname with STRYZHAK, [redacted] instructed Co-Conspirator-1 to use the nickname [redacted] had previously discussed with STRYZHAK as the login name for an account on the Nefilim panel.

(g) On or about June 23, 2021, Co-Conspirator-1 created an account for STRYZHAK to access the Nefilim ransomware panel.

(h) Also on or about June 23, 2021 [redacted] provided STRYZHAK with access to the Nefilim ransomware panel.

(i) On or about June 23, 2021, STRYZHAK accessed without authorization the network of Victim 7. STRYZHAK used WinSCP to exfiltrate files from Victim 7, including documents relating to oil and gas deliveries, such as customs documents.

(j) On or about June 28, 2021, an individual whose identity is known to the Grand Jury ("Co-Conspirator-2") notified [redacted] that Co-Conspirator-2 had successfully extorted Victim 5 for a ransom payment.

(k) On or about June 28, 2021, [redacted] and Co-Conspirator-2 determined the distribution of proceeds from the ransomware payment from Victim 5 to other co-conspirators involved in the attack against Victim 5.

(l) On or about June 29, 2021, STRYZHAK agreed to create three email accounts to serve as contact addresses for use in a Nefilim ransom note built into a customized Nefilim ransomware executable.

(m) On or about July 3, 2021, STRYZHAK agreed with [redacted] to use the Nefilim ransomware against companies located in the United States, Canada, and Australia with annual revenues above $200 million.

(n) On or about July 22, 2021, STRYZHAK informed [redacted] that he had network access to several companies, including Victim 8.

(o) Approximately five hours later, STRYZHAK, [redacted], and other Nefilim conspirators attempted to gain unauthorized access to computers used by Victim 8.

(p) From on or about September 8, 2021, to on or about October 14, 2021, [redacted] used public tracing tools to follow the cryptocurrency proceeds of Victim 5's ransom payment.

(q) On or about August 25, 2021, [redacted] was contacted by an individual who sought to assist [redacted] and his co-conspirators in conducting Nefilim ransomware attacks. [redacted] stated that he and his co-conspirators were interested in targeting companies with an annual revenue of at least $100 million located in the United States, Canada and Australia, and required the prospective co-conspirator to pay 20 percent of any ransom proceeds.

(r) On or about August 29, 2021, an individual whose identity is known to the Grand Jury ("Co-Conspirator-3") provided to [redacted] approximately 21 email accounts and their apparent associated passwords for use in ransom negotiations with victims of Nefilim ransomware.

(s) On or about September 7, 2021, [redacted] provided to an individual whose identity is known to the Grand Jury ("Co-Conspirator-4") approximately nine of the 21 email accounts previously provided to [redacted] by Co-Conspirator-3. [redacted] then requested that Co-Conspirator-4 prepare three customized Nefilim ransomware executable files. [redacted] further instructed Co-Conspirator-4 to use three of the nine provided email addresses when preparing each of customized Nefilim ransomware executable files for deployment.

(t) On or about October 24, 2021, [redacted] provided to an individual whose identity is known to the Grand Jury ("Co-Conspirator-5") the same nine email accounts that [redacted] had provided to Co-Conspirator-4.

(u) On or about October 25, 2021, Co-Conspirator-5 told [redacted] that corporate data belonging to Victim 6 had been downloaded by the co-conspirators. On or about October 25, 2021, [redacted] relayed that same message to Co-Conspirator-4.

(v) On or about October 25, 2021, [redacted] and his co-conspirators deployed Nefilim ransomware against Victim 6 and left a note on Victim 6's computers demanding that Victim 6 send an email to the perpetrators. In the note, [redacted] and his co-conspirators provided three email addresses as contact emails.

Each of the contact email addresses was included in the list of nine email addresses that [redacted] had previously shared with Co-Conspirator-4 and Co-Conspirator-5.

(w) On or about October 26, 2021, Co-Conspirator-5 sent [redacted] a response from Victim 6 confirming receipt of the ransom demand and requesting proof of extracted data.

(x) On or about October 27, 2021, [redacted] and his co-conspirators sent a ransom note to Victim 6 demanding approximately 23.5 BTC, valued at approximately $1.5 million.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

[redacted]

[redacted]

CRIMINAL FORFEITURE ALLEGATION

64. The United States hereby gives notice to the defendants that, upon their conviction of any of the offenses charged herein, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2) and 1030(i)(1), which require any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses, and such persons' interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offenses.

65. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and [redacted], to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2), 982(b)(1), [redacted] and 1030(i)(2); Title 21, United States Code, Section 853(p))

A TRUE BILL

FOREPERSON

By Carolyn Pokorny, Assistant U.S. Attorney

BREON PEACE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK